AMENDMENTS TO THE CLAIMS

The listing of claims replaces all prior versions and listings of claims. Only those claims being amended herein show their changes in highlighted form, where insertions appear as underlined text (e.g., insertions) while deletions appear as strikethrough text or brackets (e.g., deletions or [[deletions]]). Accordingly, please amend Claims 1-5 and 10-12, cancel Claims 6-9 without prejudice or disclaimer, and add new Claims 13-20 as follows:

1.   (**Currently Amended**) A [[An]] apparatus for a baseline authentication agency for determining in a global network the user a user's login status as the user accesses a goes from site to site within a said network, said apparatus comprising:

a database storing information about partner sites that have been linked by a user;

a set of baseline authentication agencies agency server responsible for core global network authentication services configured:

to receive a request from a user's browser, the request comprising:

a site identification identifying a site; and

a cookie related to the user and including a reference to the baseline authentication agency;

to determine whether the cookie is valid;

to determine whether the user has authorized seamless login for the site using the information from the database; and

to generate a login ticket for the site and send the login ticket to the user's browser if the cookie is valid and the user has authorized seamless login for the site;

wherein the cookie is stored on a global network domain and associated DNS records used for cookie sharing[[,]] login routing, and the like; and the site is one of a collection of partner sites with access to cookies shared on the via said global network domain.

2.   (**Currently Amended**) The apparatus of Claim 1, wherein the [[a]] baseline authentication agency of said set of baseline authentication agencies: provides authentication services for a subset of [[the]] users of the global network domain, the baseline authentication agency server further configured to:

after authenticating the [[a]] user, write the writes a site identification along with an authenticated status of true into the [[a]] cookie of the user stored on the [[said]] global network domain and shared and accessible by [[said]] the collection of partner sites; and after [[when]]

the ~~a global network~~ user logs out of said global network domain, reset [[resets]] the user's authenticated status to false in the [[said]] ~~shared domain~~ cookie.

3. (**Currently Amended**) The apparatus of Claim 1 [[2]], wherein the baseline authentication agency server is further ~~comprising~~ configured to:

receive the ticket from the site;

determine whether the ticket is valid; and

if the ticket is valid, send user identification information to the site, the user identification information to be used by the site to login the user.

~~means for when an authenticated global network user using a browser visits a partner site of said collection of partner sites, said partner site accessing said shared domain cookie to determine the user's baseline authentication agency;~~

~~means for said partner site redirecting said user's browser to said baseline authentication agency to request global network id informational of the user;~~

~~wherein said baseline authentication agency distinguishes between sites that have been linked and that have a trust relationship with the user and ones that have not been linked; and~~

~~means for said baseline authentication agency returning said global network id informational of the user to said partner site if it's a linked site, thereby performing a seamless authentication, and if said site is not linked, said baseline authentication agency returning an authentication error indication.~~

4. (**Currently Amended**) The apparatus of Claim 1 [[2]], wherein the baseline authentication agency server is further ~~comprising~~ configured to:

send a message to the user's browser that indicates that no ticket is available if the cookie is not valid or if the user has not authorized seamless login for the site.

~~means for when an unauthenticated global network user visits a global partner site, said global network partner site attempting to access said shared domain cookie and either not finding said cookie at all, or determining that said authenticated status is false; and~~

~~wherein in either case, said global network partner site determining that a user is not authenticated into the global network and thus not allowing access for said user.~~

5. (**Currently Amended**) The apparatus of Claim 1 [[2]], wherein the baseline authentication agency server further ~~comprising~~ comprises:

a globally unique identifier for each global network user account, wherein said globally unique identifier is a primary key with which the database is ~~global network user data records are~~ indexed, ~~and wherein for privacy reasons, only said globally unique~~

~~identifier and a name of an associated baseline authenticating agency are shared with~~
~~third party sites unless a user opts-in to distributing said global network login id.~~

6.   **(Cancelled)**

7.   **(Cancelled)**

8.   **(Cancelled)**

9.   **(Cancelled)**

10.   **(Currently Amended)**   A <u>computer-implemented</u> method for a <u>baseline</u>
<u>authentication agency that determines a user's login permission for a site,</u> ~~user on a global~~
~~network using a browser visiting a partner Web site, wherein said partner Web site is a linked~~
~~and seamlessly login enabling global network site, during an ongoing session, said~~ <u>the</u> method
<u>comprising</u> ~~the steps of~~<u>:</u>

> <u>receiving a request from a user's browser, the request comprising a site identifier</u>
> <u>related to a site, and a set of user information related to a user and including a</u>
> <u>reference designating the baseline authentication agency;</u>
> <u>determining whether the set of user information is valid;</u>
> <u>if the set of user information is valid,</u>
>> <u>determining whether the user has authorized seamless login for the site;</u>
> <u>and</u>
>> <u>generating a login ticket for the site and sending the login ticket to the</u>
> <u>user's browser if the user has authorized seamless login for the site;</u>

~~said user selecting said partner Web site and said browser requesting a home page of~~
~~said partner Web site, wherein said home page of said partner Web site comprises a~~
~~JavaScript tag telling said browser to fetch a partner site-served JavaScript file from said~~
~~partner site server, as well as fetch other relevant JavaScript code;~~

~~said partner Web site server obtains a network login status cookie on a global network~~
~~domain, thereby determining said user's global network login status and BAA;~~

~~said partner Web site using a BAA id from said network login status cookie for~~
~~formulating a URL to a login token-generation service of said associated authentication agency~~
~~domain, and returning an HTTP redirect to said URL;~~

~~said browser fetching said URL, and passing a global network site id of said partner~~
~~Web site;~~

~~said associated authentication agency domain receiving said token-generation request~~
~~including said site id, as well as any corresponding user global network credential cookie~~
~~previously sent to the browser;~~

~~said partner Web site's home page comprising a particular JavaScript code and using said particular JavaScript code for determining a JavaScript login-token variable has a value, wherein if said login-token variable has said value, then said proceeds with a seamless global network login processing;~~

~~said partner Web site requesting mapping of said login-token variable to an user global network account number;~~

~~said global network server decrypting said login-token variable and performing validation checks on said login-token variable, said checks comprising, but not limited to: not expired and if an associated IP of said requesting partner Web site is in an allowed list, and if said validation checks pass, then said global network server returning said global network account number to said partner Web site; and~~

~~said partner Web site mapping said user's global network account number to a corresponding partner Web site record, logging user in, setting cookies of said partner Web site, and returning a personalized welcome page.~~

11.   (**Currently Amended**) The method of Claim [[of]] 10 further comprising ~~the steps of~~:

~~said associated authentication agency domain~~ checking if the site [[id]] identifier is known or valid~~, if said user's credentials are valid, and if the user has authorized seamless login to said partner Web site~~.

12.   (**Currently Amended**) The method of Claim [[of]] 10, ~~said seamless global network login processing~~ further comprising ~~the steps of~~:

generating [[said]] JavaScript code writing out an HTML form comprising the ~~said global network~~ login ~~token~~ ticket as a hidden field and writing out a partner Web site global network login handler as an action URL, and auto-submitting said form such that the ~~said~~ browser posts the ~~said~~ form to a [[said]] partner Web site global network login handler URL on the ~~said~~ partner [[Web]] site.

13.   (**New**) The method of Claim 10, wherein the set of user information is a cookie.

14.   (**New**) The method of Claim 10, wherein the site is one of a collection of partner sites.

15.   (**New**) The method of Claim 10, wherein generating the login ticket for the site comprises generating JavaScript code that stores the login ticket.

16.   (**New**) The method of Claim 15, wherein sending the login ticket for the site comprises sending the JavaScript code.

17.   (**New**) The method of Claim 10, further comprising

if the set of user information is valid,

    receiving the ticket from the site;

    determining whether the ticket is valid; and

    if the ticket is valid, sending user identification information to the site, the user identification information to be used by the site to login the user.

18.   (**New**) A storage medium having a computer program stored thereon for causing a suitably programmed system to process computer-program code by performing the method of Claim 10 when such program is executed on the system.

19.   (**New**) A baseline authentication agency configured to determine a user's login permission for a site, the baseline authentication agency comprising:

    a list of partner sites that have been linked by a user;

    a baseline authentication agency server configured to:

        receive a request from a user's browser, the request comprising a site identifier related to a site, and a set of user information related to a user and referencing the baseline authentication agency;

        determine whether the set of user information is valid;

        determine whether the user has authorized seamless login for the site; and

        if the set of user information is valid and the user has authorized seamless login for the site,

            generate a login ticket for the site;

            send the login ticket to the user's browser.

20.   (**New**) The baseline authentication agency of Claim 19, wherein the baseline authentication agency server is further configured to:

    receive the ticket from the site;

    determine whether the ticket is valid; and

    if the ticket is valid, send user identification information to the site, the user identification information to be used by the site to login the user.